(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－134311

(43)公開日　平成９年(1997)５月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｂ
						３２０Ｆ
	1/00	３７０			1/00	３７０Ｅ
	15/00	３３０			15/00	３３０Ｚ

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平7－289009

(22)出願日　平成７年(1995)11月７日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　片岡　達史
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　岡田　守弘

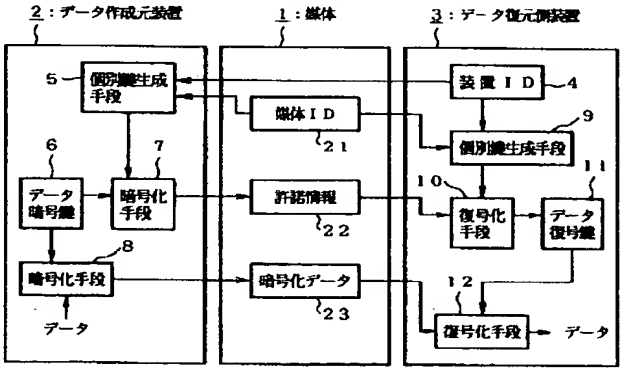
(54)【発明の名称】　機密保護システム

(57)【要約】

【課題】　本発明は、機密保護システムに関し、装置ＩＤ、媒体ＩＤ、データ暗号化鍵を用いて暗号化した許諾情報および暗号化データを媒体に書き込み、装置ＩＤを持った装置のみが復号化可能とし、媒体や復元プログラムが盗用されても暗号化データの復元を不可とし、媒体上の暗号化データの機密保護を図ることを目的とする。

【解決手段】　データの書き込み時に、媒体から読み出した媒体１Ｄと自身の装置ＩＤとデータ暗号化鍵とから暗号化した許諾情報、およびデータ暗号鍵でデータを暗号化した暗号化データを媒体に書き込み、データの読み出し時に、媒体から読み出した媒体１Ｄと許諾情報と自身の装置ＩＤからデータ復号鍵を復号し、この復号したデータ復号鍵を用いて媒体から読み出した暗号化データを復号する手段を設けた装置とからなるように構成する。

本発明のシステム構成図



1

【特許請求の範囲】

【請求項１】媒体上のデータの機密保護する機密保護システムにおいて、

媒体ＩＤ、許諾情報、および暗号化データを書き込む可搬可能な媒体と、

データの書き込み時に、上記媒体から読み出した上記媒体ＩＤと自身の装置ＩＤとデータ暗号化鍵とから暗号化した許諾情報およびデータ暗号鍵でデータを暗号化した暗号化データを上記媒体に書き込み、データの読み出し時に、上記媒体から読み出した媒体ＩＤと許諾情報と自身の装置ＩＤからデータ復号鍵を復号し、この復号したデータ復号鍵を用いて上記媒体から読み出した暗号化データを復号する手段を設けた装置とからなることを特徴とする機密保護システム。

【請求項２】媒体上のデータの機密保護する機密保護システムにおいて、

媒体ＩＤ、許諾情報、および暗号化データを書き込む可搬可能な媒体と、

データの書き込み時に、上記媒体から読み出した上記媒体ＩＤと自身の装置ＩＤから生成した個別鍵でデータ暗号化鍵を暗号化した許諾情報、およびデータ暗号鍵でデータを暗号化した暗号化データを上記媒体に書き込み、データの読み出し時に、上記媒体から読み出した媒体ＩＤと自身の装置ＩＤから生成した個別鍵で媒体から読み出した許諾情報を復号化してデータ復号鍵を生成し、この生成したデータ復号鍵で媒体から読み出した暗号化データを復号する手段を設けた装置とからなることを特徴とする機密保護システム。

【請求項３】上記装置が複数ある場合に、装置毎の装置ＩＤに対応して、上記許諾情報をそれぞれ生成して上記媒体にそれぞれ書き込んだことを特徴とする請求項１記載の機密保護システム。

【請求項４】上記媒体に書き込む暗号化データが複数ある場合に、暗号化データ毎に上記許諾情報を媒体に書き込むことを特徴とする請求項１記載の機密保護システム。

【請求項５】上記装置ＩＤとしてコンピュータ装置自身の装置ＩＤあるいは媒体に読み書きする可搬型の媒体アクセス装置の装置ＩＤとしたことを特徴とする請求項１記載の機密保護システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、媒体上のデータの機密保護する機密保護システムに関するものである。

【０００２】

【従来の技術】従来、複数の装置（端末）がホストに接続されたシステムにおいて、ある装置上で作成したデータをＭＯ（光磁気ディスク）などの媒体に書き込むと共に固有識別記号を書き込んでおき、読み出す側の装置でこの固有識別記号を入力して元のデータを読み出し、媒

2

体が何らかの原因によって紛失したときのデータの盗用を防止していた。

【０００３】

【発明が解決しようとする課題】上述したように、ある装置がデータを媒体に書き込むと共に固有識別記号を書き込んでおき、読み出し側の装置から固有識別記号を入力して媒体からデータを復元していたのでは、復元用の装置が何でもよく、復元用プログラムが媒体と一緒に盗用されてしまうと容易にデータが他の装置で復元されて非所望に使われてしまうという問題があった。

【０００４】本発明は、これらの問題を解決するため、装置ＩＤ、媒体ＩＤ、データ暗号化鍵を用いて暗号化した許諾情報および暗号化データを媒体に書き込み、装置ＩＤを持った装置のみが復号化可能とし、媒体や復元プログラムが盗用されても暗号化データの復元を不可とし、媒体上の暗号化データの機密保護を図ることを目的としている。

【０００５】

【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、媒体１は、媒体ＩＤ、許諾情報、および暗号化データを書き込む可搬可能な媒体である。

【０００６】個別鍵生成手段５は、装置ＩＤ４および媒体ＩＤ２１から個別鍵を生成するものである。暗号化手段７は、データ暗号鍵６を個別鍵で暗号化して許諾情報２２を生成するものである。

【０００７】暗号化手段８は、データをデータ暗号鍵６で暗号化して暗号化データ２３を生成するものである。個別鍵生成手段９は、装置ＩＤ４および媒体ＩＤ２１から個別鍵を生成するものである。

【０００８】復号化手段１０は、許諾情報２２を個別鍵で復号してデータ復号鍵１１を生成するものである。復号化手段１２は、暗号化データ２３をデータ復号鍵１１で復号してデータを生成するものである。

【０００９】次に、動作を説明する。データの書き込み時に、個別鍵生成手段５が媒体１から読み出した媒体ＩＤ２１と自身の装置ＩＤ４から生成した個別鍵でデータ暗号化鍵６を暗号化した許諾情報２２を生成して媒体１に書き込むと共に、暗号化手段８がデータ暗号鍵６でデータを暗号化した暗号化データ２３を媒体に書き込む。そして、データの読み出し時に、個別鍵生成手段９が媒体１から読み出した媒体ＩＤ２１と自身の装置ＩＤ４から個別鍵を生成し、復号化手段１０がこの生成した個別鍵で媒体１から読み出した許諾情報２２を復号化してデータ復号鍵１１を生成し、復号化手段１２がこの生成したデータ復号鍵１１で媒体１から読み出した暗号化データ２３を復号しデータを生成するようにしている。

【００１０】この際、装置が複数ある場合に、装置毎の装置ＩＤ４に対応して、許諾情報２２をそれぞれ生成して媒体１にそれぞれ書き込んむようにしている。また、

媒体１に書き込む暗号化データ２３が複数ある場合に、暗号化データ２３毎に許諾情報２２を媒体１に書き込むようにしている。

【００１１】また、装置ＩＤとしてコンピュータ装置自身の装置ＩＤあるいは媒体１に読み書きする可搬型の媒体アクセス装置の装置ＩＤとするようにしている。従って、装置ＩＤ、媒体ＩＤ、データ暗号化鍵を用いて暗号化した許諾情報２２および暗号化データ２３を媒体１に書き込み、装置ＩＤを持った装置のみが復号化可能とすることにより、媒体や復元プログラムが盗用されても暗号化データの復元を不可とし、媒体上の暗号化データの機密保護を図ることができる。

【００１２】

【発明の実施の形態】次に、図１から図５を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１３】図１は、本発明のシステム構成図を示す。図１において、媒体１は、一意な媒体ＩＤ、許諾情報、および暗号化データを書き込む可搬可能な媒体であって、例えばＭＯ（光磁気ディスク）などの大容量記憶できる可搬可能な媒体である。

【００１４】媒体ＩＤ２１は、媒体に書換え不可の形で一意な媒体ＩＤを書き込んだものであって、例えばレーザビームで所定領域に焼き切って一意の媒体ＩＤを書き込んだものである。これにより、媒体１をコピーしても当該媒体ＩＤがコピーできず、媒体１自身の偽造を防止できる。

【００１５】許諾情報２２は、個別鍵でデータ暗号鍵６を暗号化したものである。暗号化データ２３は、データをデータ暗号鍵６で暗号化したものであって、ＤＥＳなどの暗号アルゴリズムで暗号化したデータである。

【００１６】データ作成元装置２は、データ暗号鍵６を暗号化して媒体１に書き込んだり、データをデータ暗号鍵６で暗号して媒体１に書き込んだりなどするものであって、個別鍵生成手段５、暗号化手段７、８などから構成されるものである。

【００１７】個別鍵生成手段５は、媒体１から読み取った一意な媒体ＩＤ２１および装置ＩＤ４から個別鍵を生成するものである。ここで、装置ＩＤとしてコンピュータ装置自身の装置ＩＤあるいは媒体に読み書きする可搬型の媒体アクセス装置の装置ＩＤとしている。通常は、前者を装置ＩＤとしているが、インストール時や保守時に、可搬型の媒体アクセス装置（例えば光磁気ディスク装置）を持ち運び、制御プログラムをインストールしたり、データを格納したりするときに、１つの当該媒体アクセス装置の装置ＩＤに対応づけた許諾情報および暗号化データを媒体１に書き込んでおけば、当該１台の媒体アクセス装置を用いて全ての装置へのプログラムのインストールやデータの初期設定や修正などを行うことができ、保守作業に極めて便利である。

【００１８】暗号化手段７は、データ暗号鍵６を個別鍵で暗号化して許諾情報２２として媒体１に書き込むものである。暗号化手段８は、データ暗号鍵６でデータを暗号化し暗号化データ２３として媒体１に書き込むものである。

【００１９】データ復元側装置３は、データ復元側の装置であって、媒体１から媒体ＩＤ、許諾情報２２、暗号化データ２３を読み取って復号化してデータを生成するものであり、個別鍵生成手段９、復号化手段１０、１２などから構成されるものである。

【００２０】個別鍵生成手段９は、媒体１から読み取った媒体ＩＤと自身の装置ＩＤから個別鍵を生成するものである。復号化手段１０は、生成した個別鍵で媒体１から読み取った許諾情報を復号化しデータ復号鍵１１を生成するものである。

【００２１】復号化手段１２は、生成したデータ復号鍵１１で、媒体１から読み取った暗号化データ２３を復号してデータを生成するものである。図２は、本発明の媒体情報例を示す。

【００２２】図２の（ａ）は、媒体情報例を示す。この媒体情報は、図１の可搬可能な媒体１に書き込む情報であって、図示の下記の情報である。

・媒体ＩＤ
・企業固有ＩＤ
・許諾情報１～ｎ
・暗号化データ１～ｎ

ここで、媒体ＩＤは、既述したように、レーザビームなどで媒体上に焼き切るように媒体ＩＤを書き込んだものであって、媒体１上のデータをコピーしても複製できないものである。企業固有ＩＤは、企業固有のＩＤであって、システムが異なる企業毎に一意に決定したＩＤである。許諾情報１～ｎは、装置が異なる毎に生成したものである。従って、１つの暗号化データをｎ台の装置に例えば書き込んだり、インストールしたりするには、ｎ個の装置毎の許諾情報を書き込むこととなる。暗号化データ１～ｎは、許諾情報毎の暗号化データである。尚、複数の許諾情報に対応づけて１つの暗号化データを格納するようにしてもよい。

【００２３】図２の（ｂ）は、許諾情報と装置ＩＤとの対応づけを説明する説明図である。許諾情報は、図１で説明したように、装置ＩＤ４と媒体ＩＤ２１から個別鍵を生成し、この個別鍵でデータ暗号鍵６を暗号して生成したものである。従って、結果として、装置ＩＤに対応づけてそれぞれ許諾情報が生成されることとなるので、その様子を模式的に表したものであり、許諾情報１は装置ＩＤ１に対応し、以下同様に対応するものである。

【００２４】次に、図３のフローチャートに示す順序に従い、図１の構成の暗号化データを作成するときの手順を詳細に説明する。図３は、本発明の暗号化データ作成フローチャートを示す。

【００２５】図３において、Ｓ１は、暗号化すべきデー

タを取り出す。Ｓ２は、データ暗号鍵を取り出す。Ｓ３は、データをデータ暗号鍵で暗号化して暗号化データを作成する。

【００２６】Ｓ４は、媒体に格納する。以上によって、図１の暗号化手段８がデータ暗号鍵６を用いてデータを暗号化して生成した暗号化データ２３を媒体１に書き込むことができたこととなる。

【００２７】次に、図４のフローチャートに示す順序に従い、図１の構成の許諾情報を作成するときの手順を詳細に説明する。図４は、本発明の許諾情報作成フローチャートを示す。

【００２８】図４において、Ｓ２１は、データ復元側の装置ＩＤを取り出す。これは、データを復元する側の装置の装置ＩＤを取り出す。Ｓ２２は、媒体ＩＤを取り出す。これは、暗号化データを書き込もうとする媒体１から一意の媒体ＩＤ２１を取り出す。

【００２９】Ｓ２３は、両ＩＤにより個別鍵を作成する。これは、Ｓ２１で取り出した装置ＩＤおよびＳ２２で取り出した媒体ＩＤをもとに個別鍵を作成する。Ｓ２４は、個別鍵でデータ暗号鍵を暗号化して許諾情報を生成する。

【００３０】Ｓ２５は、媒体に格納する。Ｓ２６は、装置ＩＤの数だけ繰り返したか判別する。ＹＥＳの場合には、終了する。ＮＯの場合には、Ｓ２１に戻り繰り返す。

【００３１】以上によって、図１の個別鍵生成手段５が復元側の装置ＩＤ４および媒体１から読み取った一意の媒体ＩＤから個別鍵を生成し、暗号化手段７がこの個別鍵を用いてデータ暗号鍵６を暗号化して許諾情報２２として媒体１に書き込むことができたこととなる。

【００３２】次に、図５のフローチャートに示す順序に従い、図１の構成のデータの復号するときの手順を詳細に説明する。図５は、本発明のデータの復号化フローチャートを示す。

【００３３】図５において、Ｓ３１は、データ復元側の装置ＩＤを取り出す。これは、データを復元する側の装置の装置ＩＤを取り出す。Ｓ３２は、媒体ＩＤを取り出す。これは、暗号化データを読み出そうとする媒体１から一意の媒体ＩＤ２１を取り出す。

【００３４】Ｓ３３は、両ＩＤにより個別鍵を作成する。これは、Ｓ３１で取り出した装置ＩＤおよびＳ３２で取り出した媒体ＩＤをもとに個別鍵を作成する。Ｓ３４は、媒体上の許諾情報を個別鍵を用いて復号化してデータ復号鍵を生成する。

【００３５】Ｓ３５は、媒体上の暗号化データをデータ復号鍵を用いて復号化しデータを生成する。これは、Ｓ３１で復号しようとする装置から取り出した装置ＩＤおよびＳ３２で媒体から取り出した媒体ＩＤから個別鍵を生成し、この個別鍵を用いて媒体１上の許諾情報を復号化してデータ暗号鍵を生成し、このデータ暗号鍵を用いて媒体１から読み出した暗号化データを復号して元のデータを生成する。

【００３６】Ｓ３６は、終わりか判別する。ＹＥＳの場合には、終了する。ＮＯの場合には、Ｓ３４に戻り繰り返す。以上によって、図１の個別鍵生成手段９が復元側の装置の装置ＩＤと、媒体１から読み出した媒体ＩＤから個別鍵を生成し、復号化手段１０がこの個別鍵を用いて媒体１から読み出した許諾情報を復号化してデータ復号鍵（ここではデータ暗号鍵６と同じ）を生成し、復号化手段１２がこのデータ復号鍵を使って媒体１から読み出した暗号化データを復号して元のデータを生成することができたこととなる。

【００３７】

【発明の効果】以上説明したように、本発明によれば、装置ＩＤ、媒体ＩＤ、データ暗号化鍵を用いて暗号化した許諾情報２２および暗号化データ２３を媒体１に書き込み、装置ＩＤを持った装置のみが復号化できるようにする構成を採用しているため、媒体１や復元プログラムが盗用されても暗号化データ２３の復元を不可とし、媒体上の暗号化データの機密保護を図ることができる。

【図面の簡単な説明】

【図１】本発明のシステム構成図である。

【図２】本発明の媒体情報例である。

【図３】本発明の暗号化データ作成フローチャートである。

【図４】本発明の許諾情報作成フローチャートである。

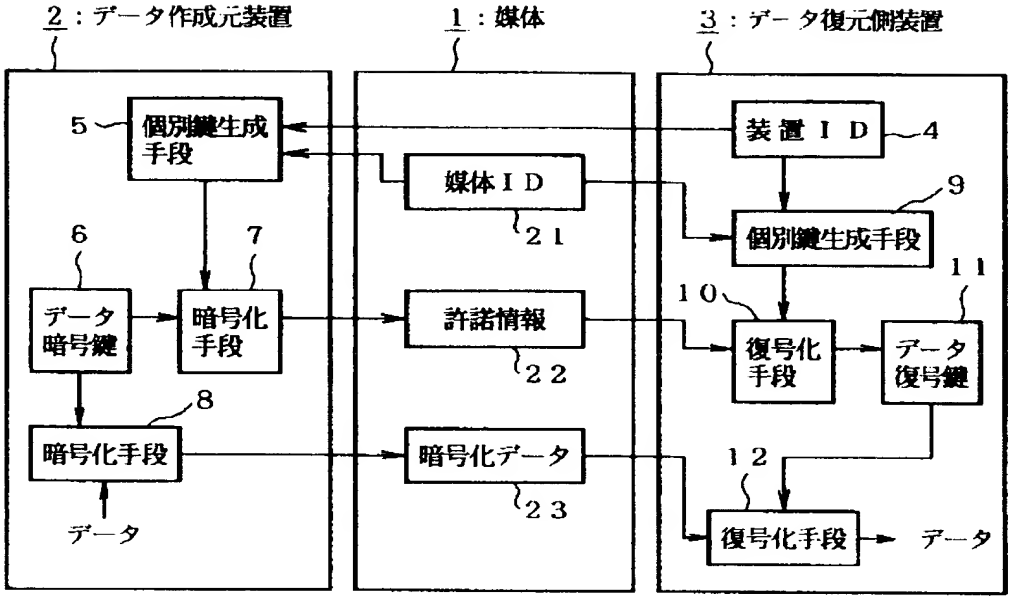
【図５】本発明のデータの復号化フローチャートである。

【符号の説明】

１：媒体
２：データ作成元装置
３：データ復元側装置
４：装置ＩＤ
５、９：個別鍵生成手段
６：データ暗号鍵
７、８：暗号化手段
１０、１２：復号化手段
１１：データ復号鍵

【図１】

本発明のシステム構成図



【図２】

本発明の媒体情報例

(a) 媒体情報

1

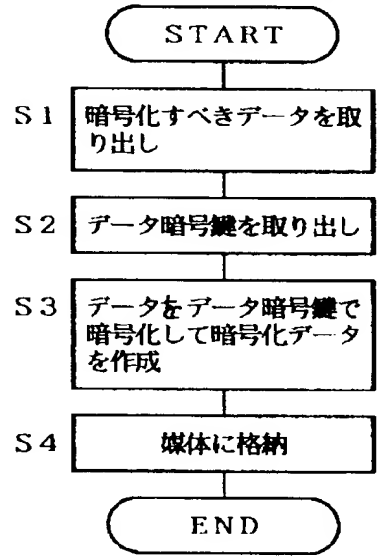
媒体ＩＤ	企業個有ＩＤ	許諾情報１～ｎ	暗号化データ１～ｎ

(b)

許諾情報１	←装置ＩＤ１
〃　２	←〃　２
〃　３	←〃　３
・ ・ ・	・ ・ ・

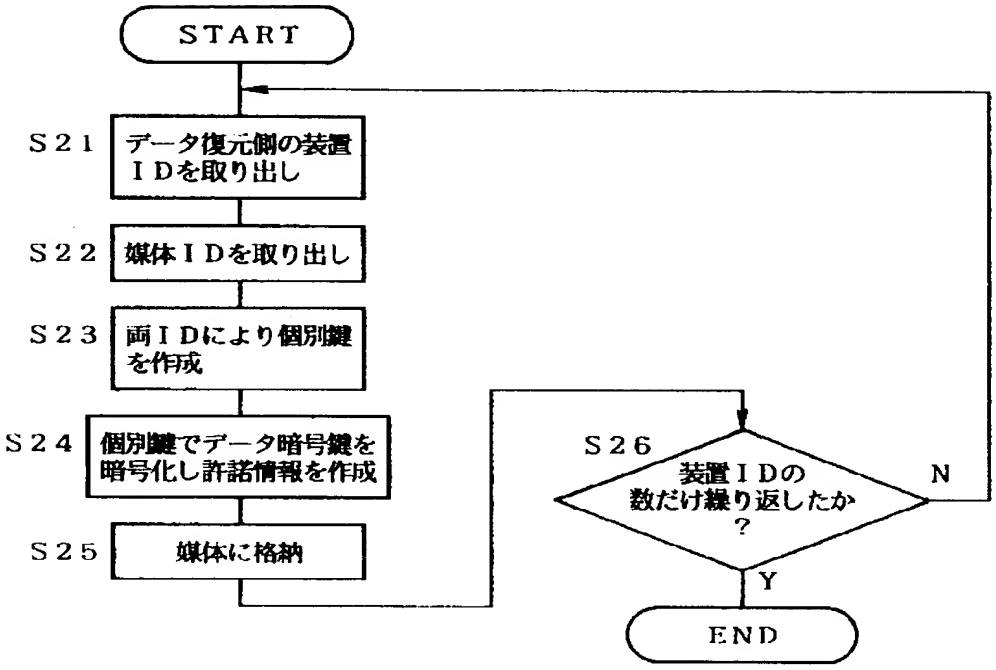
【図３】

本発明の暗号化データ作成フロ…チャ…ト



【図４】

本発明の許諾情報作成フローチャート



【図５】

本発明のデータの復号化フローチャート